

ORIENTAÇÕES GERAIS PARA CUIDAR DOS DADOS PESSOAIS

E ATENDER À LGPD NO ÂMBITO DO TCE-RN

Prezados membros, servidores, estagiários e colaboradores do TCE-RN,

Como Encarregada de Dados do Tribunal de Contas do Estado do Rio Grande do Norte, gostaria de conversar com vocês sobre um assunto que faz parte da nossa rotina, mesmo quando nem percebemos: **o cuidado com os dados pessoais.**

No nosso trabalho, diariamente temos contato com informações relacionadas a pessoas. Podemos lidar com **nome, endereço, CPF, dados bancários**, entre outros dados pessoais. Também podemos ter acesso a informações consideradas **dados pessoais sensíveis**, como dados relacionados à origem racial ou étnica, convicções religiosas, opiniões políticas e dados de saúde.

Por isso, proteger essas informações é uma responsabilidade de todos nós.

A **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)** estabelece diretrizes para o tratamento dos dados pessoais, buscando garantir o livre desenvolvimento da personalidade e a dignidade da pessoa humana. A proteção de dados pessoais também passou a fazer parte do rol dos **Direitos e Garantias Fundamentais**, por meio da Emenda Constitucional nº 115/2022, que incluiu essa proteção no art. 5º, LXXIX, da Constituição Federal.

Mas o que isso significa para nós, na prática?

Significa que precisamos incorporar alguns cuidados à nossa rotina de trabalho.

1. Vamos começar pelo básico: para que precisamos desse dado?

Quando coletamos ou utilizamos dados pessoais, precisamos ter uma finalidade legítima, específica e informada ao titular.

Também devemos observar alguns princípios importantes da LGPD:

- **Finalidade:** o tratamento deve ocorrer para finalidades legítimas, específicas e informadas ao titular;
- **Adequação:** os dados devem ser utilizados de acordo com a finalidade para a qual foram coletados;
- **Necessidade:** devemos utilizar apenas o mínimo necessário para alcançar a finalidade pretendida;
- **Transparência:** as informações sobre o tratamento devem ser claras e acessíveis ao titular;

- **Segurança:** precisamos adotar medidas para proteger os dados contra acessos não autorizados, vazamentos ou destruição;
- **Prevenção:** devemos adotar medidas para evitar danos ao titular;
- **Não discriminação:** os dados não podem ser utilizados para fins discriminatórios, ilícitos ou abusivos.

Por isso, antes de coletar ou utilizar uma informação, vale sempre fazer uma pergunta simples:

Eu realmente preciso desse dado para realizar esta atividade?

A coleta deve se limitar aos **dados pessoais essenciais para o atendimento da finalidade específica da atividade**.

2. Dados pessoais exigem cuidado e confidencialidade

Quem trabalha com dados pessoais no exercício de suas funções públicas tem responsabilidades.

A coleta e o tratamento devem ser realizados de maneira **lícita, transparente e de acordo com a finalidade específica prevista pela Administração Pública**.

Além disso, os dados pessoais devem ser mantidos em **sigilo** e ficar acessíveis apenas às pessoas autorizadas e para as finalidades permitidas pela legislação.

Quando o consentimento for necessário, deve ser obtido o consentimento expresso do titular, exceto nas hipóteses de dispensa previstas na LGPD.

Também precisamos estar atentos aos direitos dos titulares, entre eles:

- direito de acesso aos dados;
- direito de correção de dados incompletos, inexatos ou desatualizados;
- direito de exclusão dos dados, quando aplicável.

3. Cuidado com documentos, processos e impressões

Um cuidado muito simples pode evitar uma exposição desnecessária de dados pessoais: **Não deixe documentos na impressora**.

Ao imprimir documentos, processos ou procedimentos que contenham dados pessoais, procure retirá-los assim que forem impressos.

Também devemos ter precauções especiais ao **manusear e transportar documentos, processos e procedimentos**, evitando deixá-los por um longo período de tempo nas impressoras após a impressão.

4. Saiu da sua estação de trabalho? Bloqueie o computador

Quando você se ausentar do computador ou da estação de trabalho, verifique se realizou o **logout ou encerramento da sessão** em e-mails, WhatsApp, intranet e outros serviços utilizados.

Também devemos bloquear a máquina utilizando o atalho: **Windows + L**

Esse é um cuidado simples para evitar que outra pessoa tenha acesso indevido às informações enquanto você estiver ausente.

5. Quando não for necessário mostrar, proteja o dado

Outra medida importante é utilizar técnicas de **anonimização e/ou pseudonimização**, visando prevenir a identificação por terceiros e a exposição desnecessária de dados pessoais em documentos institucionais, inclusive com a aplicação de **tarjas ou asteriscos**.

O que é anonimização?

É o processo em que o agente de tratamento utiliza determinado método capaz de desvincular, de forma direta ou indireta, o dado pessoal do seu titular.

Exemplo:

Identificação:

João Silva + joao.silva@email.com + Rua A, 123, Natal/RN

Anonimização:

Cliente 001 + user002@email.com + Localização A, 123

E a pseudonimização?

É o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro, conforme o art. 13, § 4º, da LGPD.

Exemplo:

Forma incorreta:

CPF: 000.000.000-00
Matrícula: 0000000000

Forma correta:

CPF: ***.000.000.***
Matrícula: *****000

Uma ferramenta que pode ajudar

No TCE-RN, temos a ferramenta **Adélia**, que possibilita **anonimizar dados** e, assim, reduzir a exposição desnecessária de dados pessoais em documentos.

Quando precisar anonimizar um documento, você pode utilizar a ferramenta Adélia. O **tutorial com as orientações sobre como realizar a anonimização** está disponível no link abaixo:

[!\[\]\(758ebdf4629c903da74c2e079717ae32_img.jpg\) Tutorial – Anonimizador Adélia](#)

Dica: Sempre que a identificação do titular não for necessária para a finalidade do documento, avalie a possibilidade de anonimizar os dados antes de compartilhá-lo ou disponibilizá-lo.

6. Proteja também os arquivos armazenados na nuvem

Arquivos sigilosos armazenados em nuvem também precisam de proteção.

Por isso, devemos utilizar **criptografia e metodologia de senhas fortes** para proteger esses arquivos.

7. Sua senha é pessoal, sigilosa e intransferível

As senhas institucionais de acesso são, em regra, **pessoais, sigilosas e intransferíveis**.

Cada servidor é responsável por evitar sua divulgação por qualquer meio e as senhas devem ser utilizadas apenas pelos usuários cadastrados.

Por isso, a senha institucional deve ser:

- diferente daquela utilizada em aplicativos bancários;
- diferente daquela utilizada em redes sociais;
- diferente daquela utilizada em e-mails pessoais;
- diferente daquela utilizada em serviços de streaming e outros serviços.

Também deve:

- conter mais de 8 caracteres;
- incluir letras maiúsculas e minúsculas;
- incluir números;
- incluir caracteres especiais;
- não conter sequências óbvias, como “1234” ou “abcd”.

Exemplos apresentados na orientação:

Senha fraca – forma incorreta:

casa1234

Senha forte – forma correta:

M@r@t0n_2865!

8. Use autenticação de dois fatores

Sempre que estiver disponível, utilize a **autenticação de dois fatores**.

Ela é mais uma medida de proteção para os acessos institucionais.

9. Pense antes de fazer um download

Evite fazer download de arquivos que:

- sejam desnecessários para o desenvolvimento do trabalho;
- contenham dados pessoais de maneira indiscriminada;
- sejam provenientes de fontes ou sites suspeitos.

Também é importante lembrar que os **equipamentos institucionais não devem ser utilizados para fins particulares**.

10. Atenção aos e-mails, links e anexos

Ao receber um e-mail contendo links, **confira sempre o endereço do remetente**.

Também desconfie de **anexos estranhos**.

Antes de acessar um site, verifique se ele apresenta características que indiquem uma conexão segura, como:

- prefixo “**https**” no início da URL;
- ícone de cadeado na barra de endereço do navegador, indicando utilização de conexão segura **SSL/TLS criptografada**;
- domínio do site correspondente ao nome oficial da empresa, organização ou serviço.

11. E se acontecer um vazamento ou incidente?

Essa é uma orientação especialmente importante:

Em caso de vazamento ou incidente, comunique.

Se ocorrer uma situação envolvendo dados pessoais que possa caracterizar um incidente ou vazamento, a orientação é comunicar aos setores competentes para que possam ser adotadas as medidas técnicas e administrativas necessárias.

Comitê Gestor de Privacidade e Proteção de Dados – CGPD

 encarregado@tce.rn.gov.br

Diretoria de Informática

 din@tce.rn.gov.br

12. Todos nós fazemos parte da proteção de dados

A proteção de dados não depende de uma única área.

É importante que **todos os setores do Tribunal estejam plenamente engajados na confecção do mapeamento e inventário de dados**, etapa considerada relevante e indispensável para a implementação e adequação à LGPD.

Também é necessário o esforço conjunto dos setores para observar e, posteriormente, adequar os **atos normativos e institucionais, processuais e contratuais** à Lei Geral de Proteção de Dados.

Da mesma forma, cabe aos diretores fomentar práticas positivas junto às suas equipes relacionadas à **privacidade, proteção de dados e governança**.

13. Capacitação também faz parte da proteção

A participação de **membros, servidores, estagiários de graduação e pós-graduação e terceirizados** nas capacitações e ações oferecidas pelo Tribunal em conjunto com o Comitê Gestor de Privacidade e Proteção de Dados é fundamental.

A Diretoria de Informática também atua como um elo importante na **promoção e prevenção de incidentes** e na construção do Portal da LGPD no site do TCE-RN, como meio acessível para os titulares exercerem seus direitos e buscarem informações sobre o tema.

14. Por que tudo isso é tão importante?

Além das obrigações previstas na LGPD, existe a possibilidade de a **ANPD – Autoridade Nacional de Proteção de Dados**, em relação ao Poder Público, solicitar informações sobre as características dos dados, as particularidades das operações e realizar auditorias sobre o tratamento e o fluxo das informações, conforme mencionado no art. 55-J, XI e XVI.

O TCE-RN também possui normas e políticas que se relacionam com esse tema, entre elas:

- a **Resolução nº 024/2020**, que institui a Política de Gestão Documental do Tribunal de Contas do Rio Grande do Norte, com medidas e rotinas voltadas à racionalização e eficiência na criação, tramitação, classificação e avaliação de documentos, para fins de eliminação ou recolhimento para guarda permanente;

- a **Nota Técnica nº 01/2019 do Instituto Rui Barbosa**, que estabelece considerações e diretrizes sobre a aplicação da LGPD no âmbito dos Tribunais de Contas do Brasil;
- a **Lei nº 12.527/2011 – Lei de Acesso à Informação**, que consolida uma política de transparência governamental entre os órgãos públicos com o objetivo de prestação de informações à sociedade;
- a **Resolução nº 021/2021**, que instituiu a Política de Segurança da Informação no âmbito do TCE-RN, com o objetivo de observar normas técnicas, organizacionais e de gestão de riscos;
- e as normas técnicas **ISO nº 27001, nº 27002 e nº 27701**, que estabelecem padrões internacionais e disponibilizam ferramentas (framework) para a gestão da segurança da informação e da privacidade, com diretrizes para serem seguidas.

15. Cuidado: o uso indevido pode gerar responsabilização

Também é importante lembrar que existe possibilidade de **responsabilização administrativa de caráter autônomo e pessoal**, nos termos do art. 28 do Decreto-Lei nº 4.657/1942 – Lei de Introdução às Normas do Direito Brasileiro, para o servidor que infringir a LGPD.

Isso pode ocorrer, por exemplo, pelo **manuseio indevido de dados pessoais**, como modificar ou suprimir cadastros de forma inadequada, utilizar dados pessoais para fins ilegítimos e/ou vender bancos de dados.

16. Em caso de dúvida, consulte a Cartilha do CGPD

Não precisamos decorar todas as regras.

Em caso de dúvida, a orientação é fazer uso constante da **Cartilha sobre Privacidade e a LGPD**, seja em meio físico ou digital, produzida pelo Comitê Gestor de Privacidade e Proteção de Dados – CGPD.

A Cartilha é um meio de consulta e apoio para o fortalecimento da **cultura de proteção de dados no ambiente de trabalho dos diversos setores**.

Cartilha sobre Privacidade e LGPD: [Acesse a Cartilha LGPD do TCE-RN](#)

A participação de todos nas capacitações e ações de privacidade e proteção de dados também é fundamental para construirmos uma verdadeira cultura de proteção de dados no TCE-RN.

Conto com o compromisso e a colaboração de todos vocês.

Márcia Soares Marques

Encarregada de Dados – TCE-RN